REMARKS

In response to the Office Action mailed December 27, 2007, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks, have canceled claims, and have added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1-30 were pending in this Application. By this Amendment, claims 16-20 and 26-30 have been canceled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Claims 31-38 have been added. Accordingly, claims 1-15, 21-25, and 31-38 are now pending in this Application. Claims 1, 6, 11, and 21 are independent claims.

Objections

Claims 2, 7, 12, and 22 were objected to due to minor informalities. Applicants have corrected these informalities as suggested by the Office Action. No new matter has been added, and no new search is required. These amendments do not narrow or change the scope of the claims in any way, and they are supported at least by the claims as originally filed.

Rejections under §101

Claims 16-30 were rejected under 35 U.S.C. §101 for failing to fall within a statutory category of invention. Although Applicants disagree and believe that the claims were properly directed to patentable subject matter, in order to further the prosecution of this case, Applicants have canceled claims 16-20 and 26-30 and have amended claims 21-25. In particular, Applicants have amended claims 21-25 to instead recite a computer program product including a computer-

readable medium having instructions stored thereon that, when performed by a computer, cause the computer to perform various operations. No new matter has been added. Applicants wish to make it clear that these are clarifying amendments and do not narrow or change the scope of the claims in any way. Additionally, they are supported at least by the claims as originally filed.

Rejections under §102 and §103

Claims 1-15 and 21-25 were rejected under 35 U.S.C. §102(b) as being anticipated by "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics," by Mark Handley and Vern Paxson (hereinafter Handley).

Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition.

Handley teaches several methods by which a skilled attacker can evade detection by a network intrusion detection system (NIDS) by exploiting ambiguities (Pages 1-3). Handley then discloses a normalizer which is capable of altering packets to remove certain ambiguities to prevent these kinds of attacks from succeeding (Pages 3-15). In particular, one ambiguity that is discussed is the situation in which a packet arrives at a NIDS with a time-to-live (TTL) field too small to allow it to reach its destination (Page 2, Col. 1, item iii). A solution to this problem is presented according to which a packet normalizer increases the TTL of every incoming packet to a value large enough to ensure that every path within the protected network is reachable (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

Claims 1-5

Claim 1 recites a method of blocking attacks on a protected computer network. The method includes (a) receiving a plurality of packets from a network, each packet having a packet time to live (TTL) value and belonging to a corresponding packet flow, (b) storing the smallest packet TTL value received from each corresponding packet flow, and (c) prior to transmitting each packet, setting the packet TTL value to the smallest packet TTL value received for the corresponding packet flow.

The cited reference does not teach a method which includes (b) storing the *smallest packet TTL value received* from each corresponding packet flow, and (c) prior to transmitting each packet*, setting the packet TTL value to the smallest packet TTL value received for the corresponding packet flow*. Rather, Handler discloses a normalizer which **increases** the TTL of an incoming packet to a **minimum-acceptable value** in order to ensure that the packet will be able to reach any point within the internal network without timing out (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3). On the contrary, the claim discloses a very different procedure. Rather than pre-configuring a **minimum-acceptable value**, the claim requires storing the *smallest packet TTL value received* from each corresponding packet flow. Prior to transmitting each packet, the claim recites *setting the packet TTL value to the smallest packet TTL value received for the corresponding packet flow*. It is quite clear that according to the claim, the TTL value of any incoming packet is **decreased** as low as the stored *smallest packet TTL value received for the corresponding packet flow*, while according to the teaching of Handler, the TTL of an incoming packet is either **increased** up to the minimum-acceptable value, or the TTL is not modified.

For the reasons stated above, claim 1 patentably distinguishes over the cited prior art, and the rejection of claim 1 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 1 is now in allowable condition.

Because claims 2-5 depend from and further limit claim 1, claims 2-5 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Claims 6-10

Claim 6 recites an apparatus for blocking attacks on a protected computer network. The apparatus includes means for receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow. The apparatus also includes means for storing the smallest packet TTL value received from each said corresponding packet flow, as well as means for setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow prior to transmitting each said packet.

The cited reference does not teach an apparatus which includes means for *storing the smallest packet TTL value received* from each said corresponding packet flow, and means for *setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow* prior to transmitting each said packet. Rather, as mentioned above in connection with claim 1, Handler discloses a normalizer which **increases** the TTL of an incoming packet to a **minimum-acceptable value** in order to ensure that the packet will be able to reach any point within the internal network without timing out (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

Accordingly, claim 6 distinguishes over the prior art for reasons similar to those presented above in connection with claim 1.

For the reasons stated above, claim 6 patentably distinguishes over the cited prior art, and the rejection of claim 6 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 6 is now in allowable condition.

Because claims 7-10 depend from and further limit claim 6, claims 7-10 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Claims 11-15

Claim 11 recites an apparatus for blocking attacks on a protected computer network. The apparatus includes a packet classifier configured to receive a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow. The apparatus also includes a memory configured to store the smallest packet TTL value received from each said corresponding packet flow, as well as a TTL rewrite unit configured to set said packet TTL value to said smallest packet TTL value received for said corresponding packet flow prior to transmitting each said packet.

The cited reference does not teach an apparatus which includes a memory configured to *store the smallest packet TTL value received* from each said corresponding packet flow, and a TTL rewrite unit configured to *set said packet TTL value to said smallest packet TTL value received for said corresponding packet flow* prior to transmitting each said packet. Rather, as mentioned above in connection with claim 1, Handler discloses a normalizer which **increases** the TTL of an incoming packet to a **minimum-acceptable value** in order to ensure that the packet will be able to reach any point within the internal network without timing out (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

Accordingly, claim 11 distinguishes over the prior art for reasons similar to those presented above in connection with claim 1.

For the reasons stated above, claim 11 patentably distinguishes over the cited prior art, and the rejection of claim 11 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 11 is now in allowable condition.

Because claims 12-15 depend from and further limit claim 11, claims 12-15 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Claims 21-25

Claim 21 recites a computer program product including a computer-readable medium having instructions stored thereon that when performed by a computer cause the computer to perform various operations. These operations include (a) receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow, (b) storing the smallest packet TTL value received from each said corresponding packet flow, and (c) prior to transmitting each said packet, setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow.

The cited reference does not teach a computer program product which includes a computer-readable medium having instructions stored thereon that when performed by a computer cause the computer to perform operations including (b) *storing the smallest packet TTL value received* from each said corresponding packet flow, and (c) prior to transmitting each said packet, *setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow*. Rather, as mentioned above in connection with claim 1, Handler discloses a normalizer which **increases** the TTL of an incoming packet to a **minimum-acceptable value** in order to ensure that the packet will be

able to reach any point within the internal network without timing out (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

Accordingly, claim 21 distinguishes over the prior art for reasons similar to those presented above in connection with claim 1.

For the reasons stated above, claim 21 patentably distinguishes over the cited prior art, and the rejection of claim 21 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 21 is now in allowable condition.

Because claims 22-25 depend from and further limit claim 21, claims 22-25 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Newly Added Claims

Claims 31-38 have been added and are believed to be in allowable condition. Claims 31-32 depend from claim 1. Claims 33-34 depend from claim 6. Claims 35-36 depend from claim 11. Claims 37-38 depend from claim 21. Support for claims 31, 33, 35, and 37 is provided within the Specification, for example, in paragraphs [0021] and [0025]. Support for claims 32, 34, 36, and 38 is provided within the Specification, for example, in paragraphs [0021-22] and [0025]. No new matter has been added.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-128

Dated: March 27, 2008